PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-020779
(43)Date of publication of application : 23.01.1998

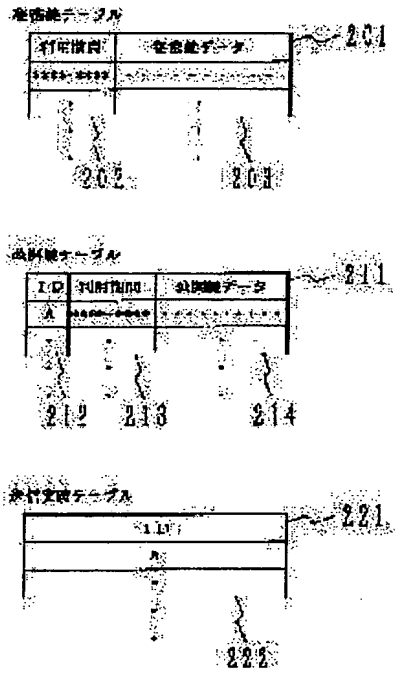
(51)Int.Cl. G09C 1/00
H04L 9/08

(21)Application number : 08-177673
(22)Date of filing : 08.07.1996

(71)Applicant : HITACHI INF SYST LTD
(72)Inventor : KOBORI MASAHIRO
SHIOMI YOSHIHIRO

(54) KEY CHANGING METHOD IN OPEN KEY CIPHER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To change a key without inconvenience by decoding encoded data and electronic signed data smoothly with a past key so as to be able to obtain transmitter authorization after the key change of an open key cipher system.
SOLUTION: This key changing method is provided with a table 201 holding past secret keys, a table 211 holding past open keys, and a table 221 holding transmitted side data before the change of keys. An old open key is transmitted to the transmitted side to which data was actually sent before the change of the key, and the data before the change of the secret key and open key is decoded on the transmitted side to confirm a signature. In decoding processing on the receiving side, whether the received data can be decoded with a present secret key or not is judged, and in the negative case, the old secret key is retrieved from the secret key table 201 to decode the data with the retrieved old secret key.



LEGAL STATUS

[Date of request for examination]	25.09.1998
[Date of sending the examiner's decision of rejection]	28.11.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－20779

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
			7259－5Ｊ			６３０Ｆ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｂ
						６０１Ｆ

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

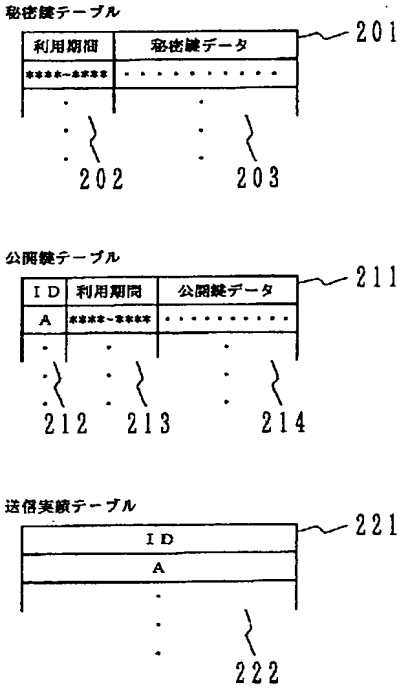
(21)出願番号　特願平8－177673

(22)出願日　平成８年(1996)７月８日

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号
(72)発明者　小堀　正裕
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(72)発明者　塩見　芳弘
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内
(74)代理人　弁理士　磯村　雅俊　（外１名）

(54)【発明の名称】　公開鍵暗号方式における鍵変更方法

(57)【要約】
【課題】公開鍵暗号方式の鍵変更後に、過去の鍵で暗号化したデータや電子署名したデータを円滑に復号し、送信者認証することができ、鍵の変更を不都合なく行う。
【解決手段】過去の秘密鍵を保持するテーブル２０１、過去の公開鍵を保持するテーブル２１１、および鍵変更以前の送信先データを保持するテーブル２２１を備え、鍵変更以前にデータを送信した実績のある送信先に旧公開鍵を送信し、それら送信先で秘密鍵および公開鍵の変更以前のデータを復号し、署名確認を行う。また、受信側の復号処理では、受信済みデータが現秘密鍵で復号可能であるか否かを判定し、不可能のとき旧秘密鍵を秘密鍵テーブル２０１を検索することにより、検索された旧秘密鍵でデータ復号を行う。



1

【 特許請求の範囲】

【 請求項1 】公開鍵暗号方式により不特定多数のコンピュータシステム間で暗号データ通信を行う場合の鍵変更方法において、

送信側および受信側のコンピュータシステムは、共に、過去の秘密鍵の履歴を保持する秘密鍵テーブル、受信した過去の公開鍵の履歴を保持する公開鍵テーブル、および暗号鍵変更以前にデータ送信した送信先I Dを保持する送信実績テーブルを備え、

暗号鍵変更時には、上記送信側コンピュータシステムから上記送信実績テーブルの送信先I Dを基に、該暗号鍵変更以前にデータ送信した送信先に旧公開鍵を送信し、

上記受信側コンピュータシステムは、受信した旧公開鍵と上記各テーブルの内容とを用いて該暗号鍵変更以前のデータを復号するとともに、送信者の署名確認を行うことを特徴とする公開鍵暗号方式における鍵変更方法。

【 請求項2 】前記旧公開鍵を受信した受信側コンピュータシステムは、他のコンピュータシステムから受信した全てのデータを格納するデータ格納ファイルを備え、

該データ格納ファイルの送信側コンピュータシステムのＩＤおよび送信日付を参照して、これらと受信した上記旧公開鍵送信コンピュータシステムのＩＤおよび使用期間とが合致するものが存在した場合には、当該公開鍵を前記公開鍵テーブルに格納し、

合致するものが存在しない場合には、受信した上記旧公開鍵を破棄することを特徴とする請求項1 に記載の公開鍵暗号方式における鍵変更方法。

【 請求項3 】前記送信側コンピュータシステムは、現用の公開鍵でデータの暗号化処理、現用の秘密鍵で署名処理を行い、日付を付加して宛先に送信すると、

前記受信側コンピュータシステムは、受信したデータを復号する場合、前記秘密鍵テーブルの利用期間から、現時点での秘密鍵の利用開始日時と、上記受信データの送信日時とを比較し、該秘密鍵の利用開始日時が上記受信データの送信日時以後であった場合には、受信データの送信日時が上記秘密鍵テーブルにおける利用期間に含まれる秘密鍵データを検索し、検索された秘密鍵データを用いて上記受信データを復号するとともに、

送信者認証を行う場合、現用の公開鍵を前記公開鍵テーブルから取得し、該公開鍵の利用開始日時と、受信データの送信日時とを比較し、公開鍵の利用開始日時が当該データの送信日時以後であった場合には、送信日時が公開鍵テーブルにおける利用期間に含まれる公開鍵データを検索し、検索された公開鍵を用いて送信者認証を行うことを特徴とする請求項1 に記載の公開鍵暗号方式における鍵変更方法。

【 発明の詳細な説明】

【０００１】

【 発明の属する技術分野】本発明は、コンピュータシステム間の公開鍵暗号方式による暗号データ通信を行う場合の暗号化鍵の変更方法に関し、特に広域ネットワーク環境下における不特定多数との間の暗号通信時において、データの暗号化と送信者の認証に好適な公開鍵暗号方式における鍵変更方法に関する。

2

【０００２】

【 従来の技術】従来より、通信内容を保護するための暗号方式としては、『秘密鍵方式』と『公開鍵方式』とがある。このうち『秘密鍵方式』は、送信者と受信者が通信内容を暗号化あるいは解読するために、同一の暗号鍵情報を保有する方法であって、暗号化および復号するための情報は当事者間しか知らされていないために、情報の秘匿性は高いが、その反面、不特定多数を対象として通信する場合（放送や同報通信）には不向きである。これに対して、『公開鍵方式』は、不特定多数の相手に通信を行う場合に向いており、例えばインターネット上での商取引を支える技術として注目されている。公開鍵方式では、暗号化された通信内容を解読するための復号情報のみを秘密鍵として非公開とし、暗号化するための暗号化情報は公開鍵として公開される。なお、秘密鍵方式、公開鍵方式の従来文献としては、例えば『暗号化電子メールＰＥＭの実装と例題』情報処理学会第４６回全国大会（菊地、森下著）、および『暗号メールの仕組みとＦＪ ＰＥＭの公開実験』平成6 年5 月３１日（黒田、菊地、山口著）等がある。

【０００３】図9 は、公開鍵方式の一般的な暗号化および復号方法を示す説明図である。図9 において、送信者Ａは受信者Ｂが公開したＢ公開鍵を用いて平文を暗号化し、暗号文を作成して受信者Ｂに送信する。一方、受信者Ｂは、自身のみが保有しているＢ秘密鍵を用いて受信した暗号文を復号して、元の平文に戻す。図１０は、公開鍵方式をコンピュータネットワークシステムで使用する場合の構成図である。ここでは、公開鍵方式をインターネットに代表されるコンピュータネットワークシステムで使用する場合を示している。図１０に示すように、暗号化するための公開鍵はサーバコンピュータに登録されており、誰からも参照、利用が可能である。一方、受信暗号文を復号するための秘密鍵は、各コンピュータで秘密に保持、管理されている。また、公開鍵暗号方式は、送信側の認証にも好適な暗号方法である。すなわち、送信側は自身の秘密鍵で認証メッセージを暗号化して、これを受信側に送信することにより、受信側は送信側の公開鍵で受信した認証メッセージを復号し、認証を行う。この場合、あるコンピュータシステムにおける秘密鍵および公開鍵は、数学的に対をなすものである。

【０００４】

【 発明が解決しようとする課題】しかしながら、秘密鍵および公開鍵の各暗号方式には、次のような問題点がある。先ず、公開鍵暗号方式では、秘密鍵が各々のコンピュータシステムで秘密に保持されることを前提にしているため、仮にこの前提が崩壊した場合には、送信側が受

3

信側の公開鍵で暗号化した暗号文は、受信側の秘密鍵を保持する全ての者に復号可能となってしまうという問題がある。また、送信側が自身の秘密鍵で認証メッセージを暗号化して、これを受信側に送信し、受信側は送信側の公開鍵で認証メッセージの復号が可能であったとしても、送信側の証明とはなり得ないという問題もある。このような場合、当該コンピュータシステムの秘密鍵および公開鍵を変更する方法が必要となる。従来は、上述のような問題点があるため、広域ネットワーク環境下における不特定多数の暗号通信に公開鍵暗号方式を用いる場合、迅速に鍵を変更することは不可能であった。一般に、1 対多数の暗号通信の場合には、事実上1 対1 の暗号通信と同等であるので、事前にコンピュータシステム間で同期をとることは容易であり、従って迅速に鍵を変更することは容易に考えられる。しかしながら、広域ネットワーク環境下では、不特定多数のコンピュータシステム間での秘密鍵および公開鍵の変更および更新の同期をとることは極めて困難であるため、安易に鍵を変更することができない。また、ある1 時点を境に鍵を変更した場合には、その1 時点以前に受信した暗号文は新規秘密鍵では復号することができず、また1 時点以前に受信した認証メッセージは新規公開鍵では認証不可能となる等の問題が生じる。そこで、本発明の目的は、これら従来の課題を解決し、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化および送信者認証を行い、迅速に公開鍵および秘密鍵の変更が可能であり、かつ鍵の変更を不都合なく行うことが可能な公開鍵暗号方式における鍵変更方法を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するため、本発明の公開鍵暗号方式における鍵変更方法では、各コンピュータシステムに、過去の秘密鍵とその属性を保持するテーブル(秘密鍵テーブル) と、過去の公開鍵とその属性を保持するテーブル(公開鍵テーブル) と、鍵変更最終時点以前の送信実績とその属性に関するデータを保持するテーブル(送信実績テーブル) とを備え、暗号鍵を変更した時点で、送信側コンピュータシステムから送信実績テーブルを基に鍵変更最終時点以前の既送信先に旧公開鍵を送信し、受信側コンピュータシステムは、受信した旧公開鍵の属性により、その旧公開鍵の要または不要の判定を行い、旧公開鍵の蓄積または破棄を確定し、蓄積する場合には、旧公開鍵とその属性を保持するテーブル(公開鍵テーブル) に格納する。そして、格納された公開鍵に対応する旧秘密鍵を秘密鍵テーブルから検索することにより、検索された旧秘密鍵でデータを復号することができる。旧公開鍵の要、不要の判定には、上記公開鍵テーブルが参照される。これにより、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認することが可能となる。さらに、ローカルに

4

公開鍵を保持している場合にも、その変更のタイミングを自動的に通知することが可能となる。

【０００６】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図1 は、本発明の一実施例を示す公開鍵暗号方式を適用するコンピュータシステムの全体構成図である。図1 において、１０１はデータを送信する送信側コンピュータＡ、１１１はデータを受信する受信側コンピュータＢである。また、１０２，１１２は後述(図2 参照) するようなシステムで利用する各テーブルを格納した鍵管理ファイル、１０３，１１３は他のコンピュータシステムから受信したデータを格納するデータ格納ファイル、１０４，１１４はコンピュータＡまたはＢで動作する暗号化プログラム、１０５，１１５は鍵管理ファイル１０２，１１２の各テーブルを用いることにより、秘密鍵および公開鍵の管理および変更時における処理を行う鍵管理プログラムである。送信側および受信側の各コンピュータ１０１，１１１は、ともに過去の秘密鍵、鍵変更以前の送信先データをテーブルに保持しているので、このテーブルを参照することにより、暗号化鍵を変更する場合には、鍵変更以前にデータを送信した実績のある送信先へ旧公開鍵を送信し、受信側のコンピュータ１１１では、受信した旧公開鍵と、上記データ格納ファイル１１３および上記鍵管理ファイル１１２の各テーブルを参照して、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認する。これにより、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化し、かつ送信者認証することができる。

【０００７】図2 は、本発明における鍵管理ファイルを構成する各テーブルのフォーマット図である。図2 において、２０１は鍵管理ファイルの内容のうち、コンピュータＡにおける過去の秘密鍵を格納する秘密鍵テーブルであって、２０２は該当する秘密鍵の使用期間を年月日分秒で示し、２０３は当該秘密鍵のデータを示している。また、２１１は鍵管理ファイルの内容のうち、他のコンピュータシステムから受信した過去の公開鍵を格納する公開鍵テーブルであって、２１２は当該公開鍵を所有していたコンピュータのＩＤを示し、２１３は当該公開鍵の使用期間を年月日分秒で示し、２１４は当該公開鍵のデータを示している。また、２２１は鍵管理ファイルの内容のうち、鍵変更最終時点以前の送信先属性を格納する送信実績テーブルであって、２２２は送信先属性として送信先コンピュータのＩＤを示している。ここでは、コンピュータ１０１のＩＤをＡ、コンピュータ１１１のＩＤをＢとしている。

【０００８】図3 は、旧公開鍵のフォーマットおよび受信データのフォーマットを示す図である。ここでは、コンピュータＡが送信する旧公開鍵のフォーマット３１１と、コンピュータＢの受信データ格納ファイルに格納さ

5

れている受信データフォーマット３０１が示されている。（ａ）の受信データフォーマットにおいて、３０２は送信先コンピュータのＩＤ、３０３は送信日時、３０４は受信済みのデータである。また、（ｂ）の旧公開鍵フォーマットにおいて、３１２は公開したコンピュータのＩＤ、３１３はこの公開鍵が利用されていた期間、３１４は旧公開鍵データである。鍵変更時に、送信側コンピュータシステムＡから旧公開鍵を送信すると、受信側コンピュータシステムＢでは、受信した（ｂ）の旧公開鍵フォーマットの利用期間と、（ａ）の受信データ格納ファイルフォーマットの送信日時を比較して、一致したものがあるか否かを判別し、あればその旧公開鍵を公開鍵テーブルに格納する。

【０００９】次に、鍵管理プログラムの鍵変更処理および旧公開鍵受信時処理の動作について説明する。図4は、コンピュータＡで動作する鍵管理プログラムの鍵変更処理の動作フローチャートであり、図5は、コンピュータＢで動作する鍵管理プログラムの旧公開鍵受信時処理の動作フローチャートである。図4に示すように、コンピュータＡにおける鍵変更時には、ステップ４０１で旧秘密鍵をコンピュータＡの秘密鍵テーブル２０１に追加して保存し、ステップ４０２で送信実績テーブル２２１を参照して、鍵変更最終時点以前のデータ送信先であるコンピュータ（ＩＤ２２２により識別）に対して旧公開鍵を送信する（ここでは、コンピュータＢに送信）。次に、図5に示すように、ステップ５０１で旧公開鍵３１１を受信したコンピュータＢは、ステップ５０２において、受信データ格納ファイル１１３に格納されている受信データフォーマット３０１の送信コンピュータのＩＤ３０２および送信日付３０３を参照して、受信した旧公開鍵送信コンピュータＩＤ３１２および使用期間３１３と合致するものが存在するか否か判定し、存在した場合には、ステップ５０３でコンピュータＢの公開鍵テーブル２１１に追加し、保存する。追加、保存された旧公開鍵に対応する旧秘密鍵を秘密鍵テーブル２０１から検索して、検索した旧秘密鍵でデータを復号することができる。また、合致するものが存在しない場合には、ステップ５０４において即座に受信した旧公開鍵を破棄する。

【００１０】次に、本発明における暗号化および復号の各処理について詳述する。図6は、コンピュータＡで動作する暗号化プログラムの動作フローチャートであり、図7は、コンピュータＢで動作する復号処理の動作フローチャートであり、図8は、図7における送信者認証処理の動作フローチャートである。いまコンピュータＡからコンピュータＢに対して暗号データを送信する場合、図6に示すように、ステップ６０１で現用の公開鍵を用いて暗号化処理を行い、ステップ６０２で現用の秘密鍵を用いて電子署名処理を行う。さらに、ステップ６０３でコンピュータＡのＩＤおよび送信日付をデータ格納ファイル３０１と同一フォーマットとなるように付加し、ステップ６０４で宛先に送信処理を行う。次に、コンピュータＢにおいて、コンピュータＡからの受信データを復号する場合、図7に示すように、ステップ７０１において受信データ格納ファイル１１３より該当データを参照し、ステップ７０２でコンピュータＢにおける秘密鍵テーブル２０１の利用期間２０２から、現時点での秘密鍵の利用開始日時と、コンピュータＢ内の受信データ格納ファイル１１３に格納されたデータフォーマット３０１の該当データにおける送信日時３０３とを比較し、秘密鍵の利用開始日時が受信データの送信日時以後であった場合には、この秘密鍵では復号できない。そこで、この場合には、ステップ７０３で、受信データの送信日時がコンピュータＢ内の秘密鍵テーブル２０１における利用期間２０２に含まれる秘密鍵データ２０３を検索し、そのデータを参照してステップ７０４でこれを復号する。さらに、ステップ７０５において、現用の公開鍵で認証メッセージを復号することにより送信者認証処理を行う。

【００１１】この送信者認証処理の詳細は、図8に示されている。図8のステップ８０１でコンピュータＡの現在の公開鍵を公開鍵テーブル２１１から取得し、ステップ８０２でコンピュータＡの現時点での公開鍵の利用開始日時と、コンピュータＢ内の受信データ格納ファイル１１３に格納された該当データフォーマット３０１の送信日時３０３とを比較し、公開鍵の利用開始日時が当該データの送信日時以後であった場合、この公開鍵では送信者認証を行うことはできない。そこで、ステップ８０３では、送信日時がコンピュータＢ内の公開鍵テーブル２１１におけるコンピュータＩＤがコンピュータＡであり、利用期間２１３に含まれる公開鍵データ２１４を検索し、検索された公開鍵を用いて、ステップ８０５で送信者認証処理を行う。しかし、送信者認証可能なデータ、つまり受信済みデータ中に、受信公開鍵利用期間と送信日時とが一致するデータが受信データ格納ファイル１１３の格納済みデータ内になければ（ステップ８０４）、ステップ８０６で即座に公開鍵テーブル２１１内の当該公開鍵を破棄する。なお、ステップ８０２において、当該受信済みデータが現公開鍵で署名確認することが可能である場合には、ステップ８０５で現公開鍵を用いて送信者認証処理を行う。

【００１２】このように、本発明においては、送信側および受信側のコンピュータシステムが共に過去の秘密鍵を保持するテーブルと鍵変更以前の送信先データを保持するテーブルを備え、送信側コンピュータが鍵を変更する時点で、これらのテーブルを基に鍵変更以前にデータを送信した実績のある送信先に旧公開鍵を送信し、秘密鍵および公開鍵を変更する以前のデータを復号化および署名確認する。これにより、公開鍵暗号方式において、過去の鍵で暗号化したデータおよび電子署名したデータ

6

7

を、鍵変更後に円滑に復号化および送信者認証を行うことができる。その結果、鍵の変更を不都合なく行うことができる。

【００１３】

【発明の効果】以上説明したように、本発明によれば、過去の鍵で暗号化したデータおよび電子署名したデータを、鍵変更後に円滑に復号化および送信者認証を行うので、迅速に公開鍵および秘密鍵の変更が可能であり、かつ鍵の変更を不都合なく行うことが可能である。

【図面の簡単な説明】

【図1】本発明の一実施例を示す公開鍵暗号方式を適用したコンピュータシステムの全体構成図である。

【図2】図1における鍵管理ファイルに格納されたテーブルフォーマット図である。

【図3】図1におけるデータ格納ファイルに格納されている受信データフォーマットおよび鍵を変更したコンピュータが送信する旧公開鍵のフォーマットの図である。

【図4】図1における鍵管理プログラムの鍵変更処理の動作フローチャートである。

【図5】図1における鍵管理プログラムの旧公開鍵受信時処理の動作フローチャートである。

【図6】図1における暗号化プログラムの動作フローチャートである。

8

【図7】本発明における復号処理の動作フローチャートである。

【図8】図7における送信者認証処理の動作フローチャートである。

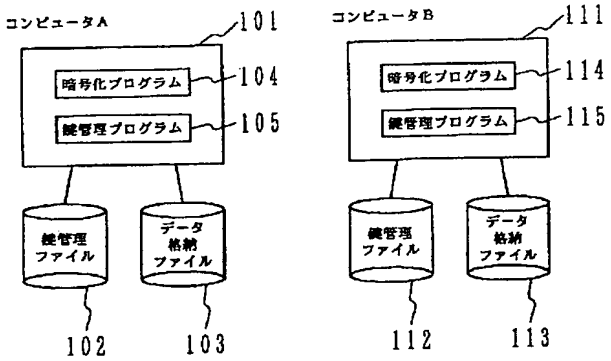
【図9】従来の公開鍵暗号方式の暗号化および復号の処理方法を示す全体構成図である。

【図10】従来の公開鍵暗号方式をコンピュータネットワークシステムで使用する場合の機能ブロック図である。

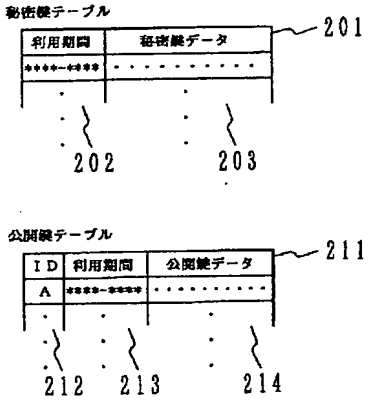
【符号の説明】

１０１…データ送信側コンピュータＡ、１１１…データ受信側コンピュータＢ、
１０２，１１２…鍵管理ファイル、１０３，１１３…データ格納ファイル、１０４，１１４…暗号化プログラム、１０５，１１５…鍵管理プログラム、２０１…秘密鍵テーブル、２０２…秘密鍵の利用期間、２０３…秘密鍵データ、
２１１…公開鍵テーブル、２１２…コンピュータのＩＤ、２１３…公開鍵の利用期間、２１４…公開鍵データ、２２１…送信実績テーブル、２２２…送信先コンピュータのＩＤ、３０１…受信データフォーマット、３１１…旧公開鍵のフォーマット。

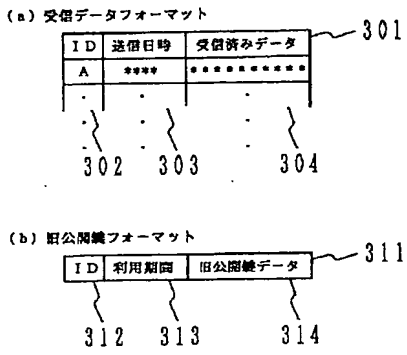
【図1】

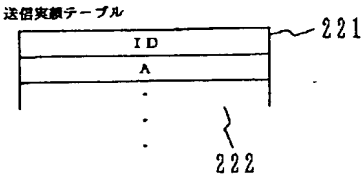


【図2】

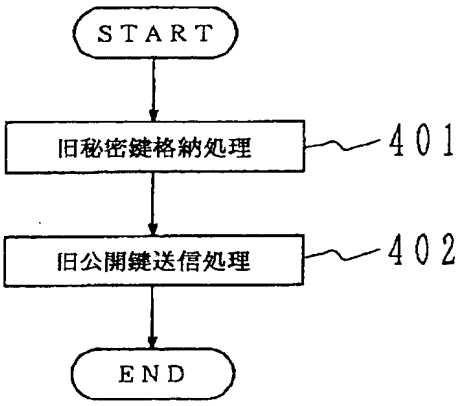


【図3】

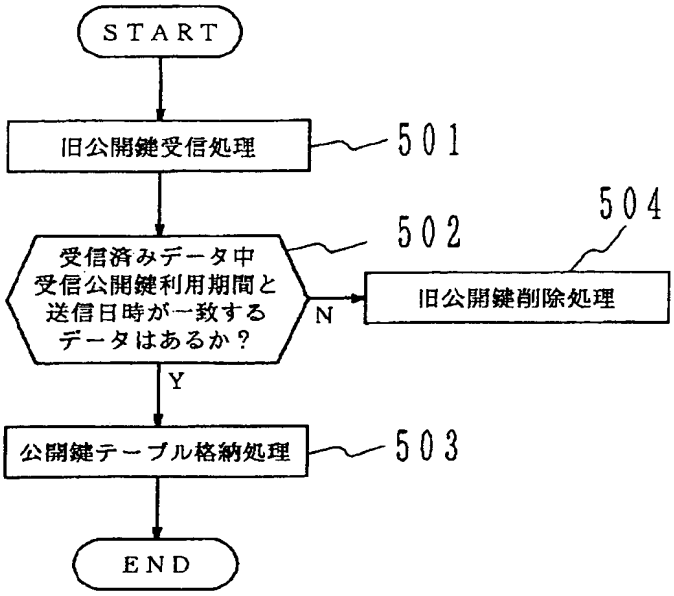




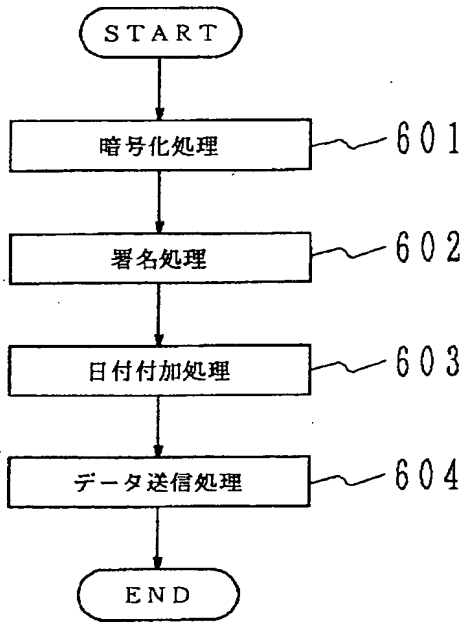
【 図4 】


START
旧秘密鍵格納処理
401
旧公開鍵送信処理
402
END

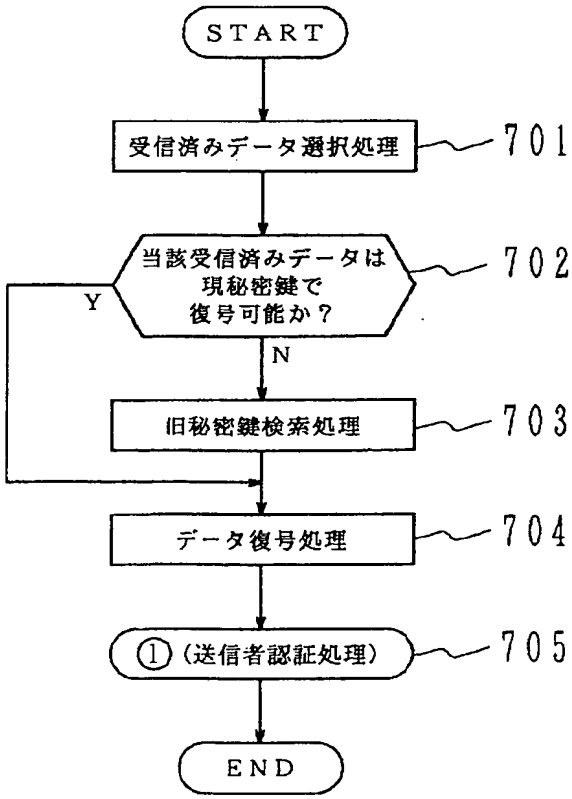
【 図5 】


START
旧公開鍵受信処理
501
受信済みデータ中
受信公開鍵利用期間と
送信日時が一致する
データはあるか？
502
N
504
旧公開鍵削除処理
Y
公開鍵テーブル格納処理
503
END

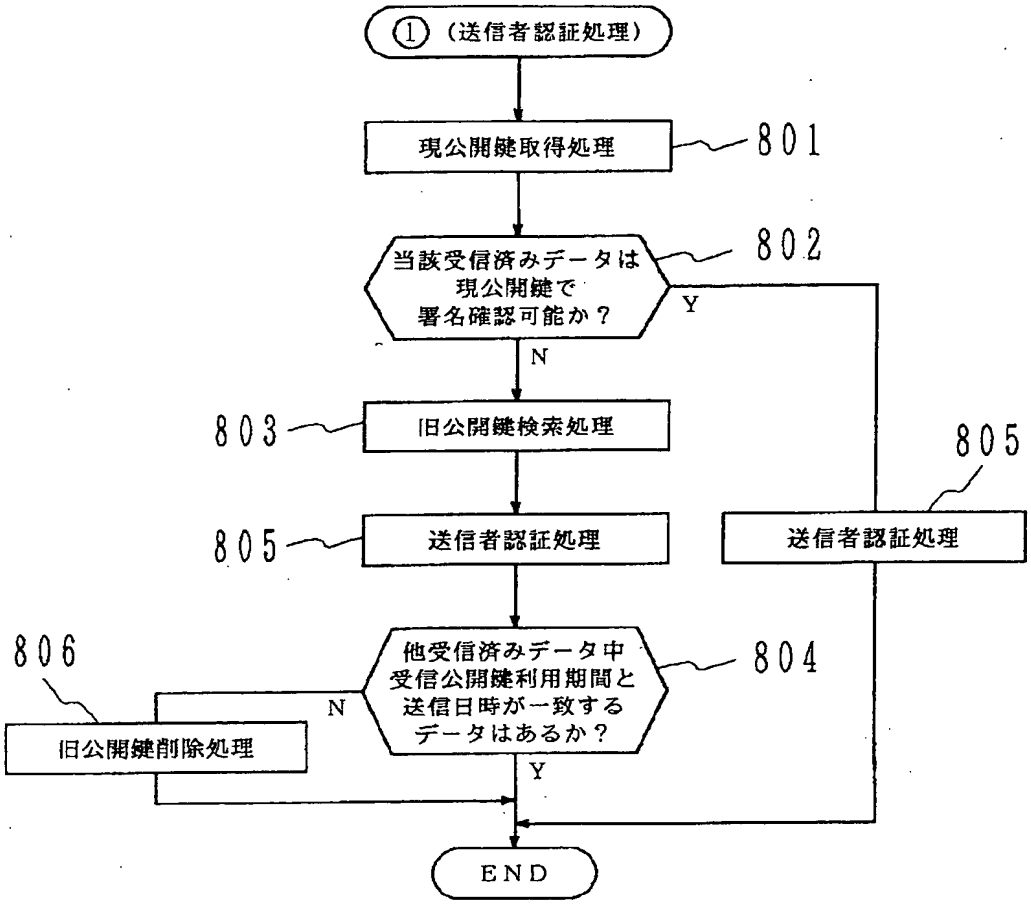
【 図6 】


START
暗号化処理
601
署名処理
602
日付付加処理
603
データ送信処理
604
END

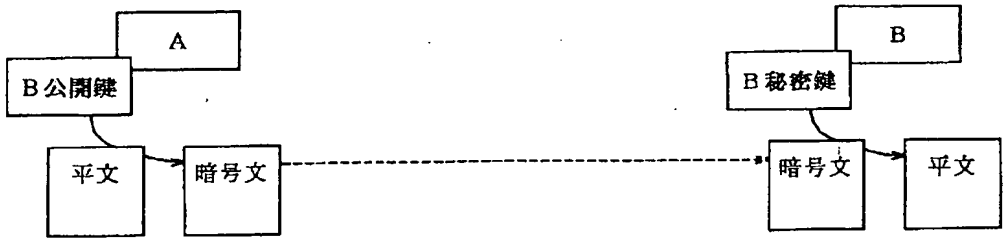
【 図7 】


START
受信済みデータ選択処理
701
当該受信済みデータは
現秘密鍵で
復号可能か？
702
Y
N
旧秘密鍵検索処理
703
データ復号処理
704
①（送信者認証処理）
705
END

【 図8 】


① (送信者認証処理)
現公開鍵取得処理
801
当該受信済みデータは
現公開鍵で
署名確認可能か？
802
Y
N
803
旧公開鍵検索処理
805
送信者認証処理
805
送信者認証処理
806
他受信済みデータ中
受信公開鍵利用期間と
送信日時が一致する
データはあるか？
804
N
旧公開鍵削除処理
Y
END

【 図9 】


A
B公開鍵
平文
暗号文
B
B秘密鍵
暗号文
平文

【 図１０ 】